Method and system for the secure transmission and storage of protectable information

Patent Number: EP0821326, A3
Publication date: 1998-01-28
Inventor(s): WITZEL MARTIN (DE); DEINDL MICHAEL (DE)
Applicant(s): IBM (US)
Requested Patent: DE19629856
Application Number: EP19970111514 19970708
Priority Number(s): DE19961029856 19960724
IPC Classification: G07F7/10; G06K17/00; G06K19/073
EC Classification: G07F7/10D10, G07F7/10D4E, G07F7/10D16
Equivalents: CN1086882B, CN1179658, JP10198606, JP3273499B2, KR269527, TW380242, US6031910
Cited Documents: EP0661675; EP0668578; EP0434550; FR2680258; DE3809795; US4672182

Abstract

The present invention describes a method and system for the secure transmission and storage of protectable information, in particular, of patient information, by means of a patient card. The data stored on the patient card are protected by cryptographic methods. The data can be decrypted only with the same patient card if a doctor is authorised and the patient has given his agreement. All information which the patient card needs in order to decide whether the doctor is authorised and the key for protecting the control data and the random key are held on the chip. The patient data can be freely transmitted to any storage medium. The chip controls both the access to the data and the encryption and decryption functions. Random keys, which are themselves stored encrypted together with the data ensure that every data record remains separate from every other and that only authorised persons can access it. Every patient card has its own record key. The system and method in accordance with the invention is not directed exclusively to patient data but can be applied to any protectable data to which right of access is to be restricted. 

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 29 856 A 1**

(51) Int. Cl.[6]: G 06 K 19/073

(21) Aktenzeichen: 196 29 856.3
(22) Anmeldetag: 24. 7. 96
(43) Offenlegungstag: 29. 1. 98

DE 196 29 856 A 1

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Schäfer, W., Dipl.-Ing., Pat.-Anw., 70188 Stuttgart

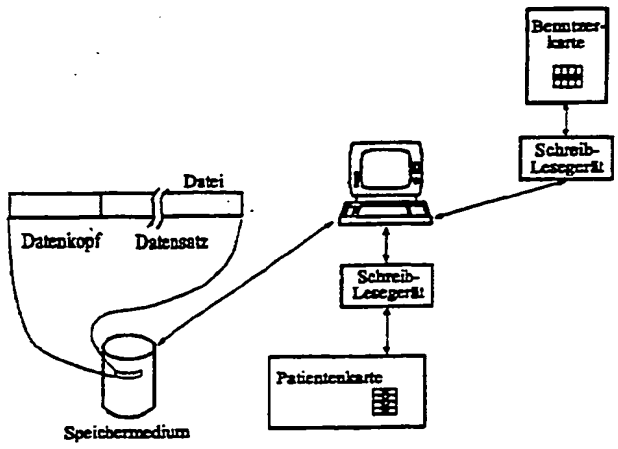
(72) Erfinder:
Deindl, Michael, 71034 Böblingen, DE; Witzel, Martin, 71101 Schönaich, DE

(56) Entgegenhaltungen:
DE 38 09 795 C2
DE 31 22 534 C1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und System zum sicheren Übertragen und Speichern von schützbaren Informationen

(57) Die vorliegende Erfindung beschreibt ein Verfahren und System zum sicheren Übertragen und Speichern von schützbaren Informationen, insbesondere von Patienteninformation mittels einer Patientenkarte. Die auf der Patientenkarte gespeicherten Daten werden durch kryptographische Methoden geschützt. Nur dieselbe Patientenkarte kann die Daten wieder entschlüsseln, wenn sich ein Arzt authentisiert und der Patient zugestimmt hat. Alle Informationen, die die Patientenkarte braucht, um zu entscheiden, ob der Arzt authentisiert ist, und die Schlüssel zum Schutz der Verwaltungsdaten und Zufallsschlüssel sind im Chip enthalten. Die Patientendaten können frei auf jedes Speichermedium übertragen werden. Der Chip kontrolliert sowohl den Zugriff auf die Daten als auch die Ver- und Entschlüsselungsfunktionen. Zufallsschlüssel, die ihrerseits zusammen mit den Daten verschlüsselt gespeichert werden, stellen sicher, daß jeder Datensatz vom anderen getrennt bleibt und daß nur autorisierte Personen zugreifen können. Jede Patientenkarte hat ihren eigenen Satz Schlüssel. Das erfindungsgemäße System/Verfahren ist nicht nur auf Patientendaten gerichtet, sondern kann auf alle schützenswerten Daten angewandt werden, auf die ein eingeschränktes Zugriffsrecht eingeräumt werden soll.



DE 196 29 856 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren und System zum sicheren Übertragen und Speichern von schützbaren Informationen, insbesondere von Patienteninformationen mittels eines Patientenkartensystems.

Patientenkartensysteme sollen vor allem den Interessen des Patienten dienen. Die personenbezogenen medizinischen Daten eines Menschen, die auf der Patientenkarte gespeichert sind, sind besonders sensitiv und daher schützenswert. Außerdem befinden sich Patienten oft in einer schwächeren Position und können ihre Schutzbelange nicht nachdrücklich vertreten. Deshalb müssen Gesetze und Vereinbarungen über den Ablauf verabschiedet werden, um die legalen und technischen Rahmenbedingungen zu schaffen, die es dem Patienten gestatten, die sensitiven Karten zu schützen.

Chipkarten bieten alle erforderlichen Kontrollmechanismen an, mit denen die Daten im nichtflüchtigen Speicher auf auf dem Chip geschützt werden. Einerseits ist der Chip gegen physische Angriffe von außen wirksam geschützt, andererseits überwacht ein Betriebssystem alle Zugriffe auf die Daten und weist Lese- und/oder Schreibversuche zurück, wenn sich der Benutzer nicht authentisieren kann und/oder eine Benutzerkennung (PIN) eingeben kann. Der Chip verhindert also, daß man von außen über seine Datenleitungen irgendwelche geschützten Daten auslesen kann. Chipkarten werden wegen ihrer anerkannt hohen Sicherheit vor allem im Finanzbereich als Identifikationssystem eingesetzt.

Der optische Speicher der Optical Memory Chip Card verwendet eine den bekannten CDs oder CD-ROMS verwandte Technologie. Sie sind wegen ihrer hohen Speicherkapazität für die Speicherung größerer Datenmengen besonders gut geeignet. Ein Nachteil dieser Speicher besteht jedoch darin, daß es keinen physischen Schutz der Daten gibt; jeder der ein geeignetes Lesegerät besitzt, kann die Daten lesen. Trotzdem kann man die Daten logisch Schützen, indem die Daten verschlüsselt gespeichert werden. Die Verschlüsselung von Daten wird auch mit dem Fachbegriff "Kryptographie" bezeichnet.

Das Problem aller symmetrischen Verschlüsselungsverfahren ist die geheime Schlüsselverteilung zwischen den beteiligten Parteien. Je größer die Zahl der Teilnehmer ist, die miteinander kommunizieren wollen, desto unüberwindlicher gestaltet sich das Problem der Schlüsselverwaltung. Es wäre leicht zu lösen, wenn alle Beteiligten den gleichen Schlüssel verwenden würden; dann könnten aber alle gegenseitig lesen, was zwei Teilnehmer einander verschlüsselt übermitteln, und im Falle eines erfolgreichen Angriffs von außen auf diesen einen Schlüssel wäre das gesamte System offen. Wenn jeder Teilnehmer seinen eigenen Schlüssel verwenden würde, bliebe ein erfolgreicher Angriff auf einen Schlüssel auf die Nachrichten beschränkt, die dieser eine Schlüsselinhaber sendet und empfängt. Die anderen Schlüsselinhaber bleiben geschützt.

Das Problem des Schlüsselaustauschs ist noch problematischer, wenn es nicht um einen Sender und mehrere Empfänger geht, es sich also um eine 1 zu N-Beziehung handelt, sondern wenn es sich um eine n zu N-Beziehung handelt. Beispielsweise kann jeder Arzt Sender einer Information sein, und jeder beliebige andere authorisierte Arzt muß sie lesen können. Wie bereits dargelegt worden ist, sollten die Ärzte auf keinen Fall einen im gesamten System benutzten Schlüssel vereinbaren dürfen, bevor sie die Kommunikation aufnehmen. Andererseits steht nicht zu erwarten, daß alle teilnehmenden Ärzte anfangs gegenseitig ihre Schlüssel austauschen.

Die Europäische Patentschrift EP 0668 578 beschreibt ein Speicher- und selektives Informationssystem für die Übertragung von sensiblen Daten bestehend aus einer optischen Speicherkarte, auf der ein räumlich definiertes Speicherfeld für die ausschließliche Speicherung einer Vielzahl von mindestens je einem Schlüsselbegriff zugeordneter Codes, mindestens einem Lese- und Schreibgerät für die optische Speicherkarte mit einer Vielzahl von Schlüsselerkennungsfunktionen, wobei je eine Schlüsselerkennungsfunktion auf je eine von einer Vielzahl in dem Schreib-/Lesegerät enthaltenen Formatierungsfunktionen verweist, und diese im Zusammenwirken mit dem jeweils zugeordneten Code aktiviert, wobei jede Formatierungsfunktion auf ein Datenspeicherfeld der optischen Karte verweist und aufgrund der dazugehörenden Formatangaben zum Lesen der dort gespeicherten Daten qualifiziert. Ein Nachteil dieses Verfahrens besteht darin, daß es einen Schlüsselbereich und einen Datenbereich auf dem optischen Speichermedium gibt. Es sind daher zwei unabhängige Zugriffe auf das optische Speichermedium notwendig um den Schlüssel und die Daten zu lesen. Das in EP 0668 578 beschriebene Verfahren verwendet feste Schlüssel, d. h. die Schlüssel werden nach einem bestimmten Verfahren vom System vorgegeben. Das Schreib-/Lesegerät ist wesentlicher Bestandteil für die Entscheidung, welcher Schlüssel verwendet werden soll. Das hängt vom Code, den Formatisierungsfunktionen und den Entscheidungsfunktionen ab. Im übrigen beschränkt sich das vorliegende Verfahren nur auf optische Speichermedien.

Es ist daher Aufgabe der vorliegenden Erfindung ein System und Verfahren zur Übertragung von schützenswerten Informationen vorzuschlagen, das einen maximalen Austausch der schützenswerten Informationen zwischen einer Vielzahl von Benutzern zuläßt, jedoch hierbei sicherstellt, daß das System/Verfahren die Eingabe als auch das Lesen der schützenswerten Informationen nur den Benutzern erlaubt, die hierfür autorisiert sind.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Vorteilhafte Ausführungsformen der vorliegenden Erfindung sind in den Unteransprüchen niedergelegt.

In der vorliegenden Erfindung werden die verschlüsselten Daten und der dazugehörige Schlüssel zusammen in einer Datei gespeichert. Dadurch können die verschlüsselten Daten unabhängig vom Speichermedium, in dem sie anfänglich niedergelegt worden sind, ohne Sicherheitsrisiko überall hin gespeichert werden, z. B. in einem Computer, in einer Datenbank oder können über ein Netzwerk verteilt werden. Innerhalb der Datei können Datentypen unterschiedlicher Geheimhaltungsstufen niedergelegt werden, deren Lesen oder Schreiben nur mit bestimmten Zugangsberechtigungen möglich ist. Die Daten werden mit einem Zufallsschlüssel verschlüsselt abgespeichert. Der Zufallsschlüssel seinerseits wird in der Chip-Karte verschlüsselt und mit den Daten abgespeichert. Dadurch wird ein systematisches Entschlüsseln der Daten wesentlich erschwert. Die Schlüsselerzeugung erfolgt ausschließlich auf der Chip-Karte. Der Berechtigte hat daher immer die volle Kontrolle über den Zugriff zu seinen Daten.

Im folgenden wird ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung an Hand von Zeichnungen näher dargestellt und erläutert, wobei

Fig. 1 eine schematische Darstellung der erfindungsgemäßen Dateistruktur und

Fig. 2 ein Flußdiagramm des Lese-und Schreibvorgangs in dem erfindungsgemäßen Informations-und Übertragungssystem zeigt.

Fig. 3 die Funktionsweise des erfindungsgemäßen Informations- und Übertragungssystems an Hand der erforderlichen Hardware zeigt.

Fig. 1 zeigt den Aufbau der erfindungsgemäßen Dateistruktur bestehend aus dem Datenkopf und dem Datensatz. Der Datenkopf besteht beispielsweise aus den Verwaltungsdatenfelder 1—7. Der Datensatz kann aus mehreren Datentypen 1-n bestehen, die im Datensatz niedergelegt sind. Jedem Datentyp ist mit einem eigenen Zufallsschlüssel verschlüsselt. Diese Zufallsschlüssel und ein Teil der Verwaltungsdaten, der geschützt werden soll, werden ihrerseits mit einem festen, auf der Chipkarte gespeicherten Schlüssel verschlüsselt. Die Chipkarte selbst verschlüsselt die Verwaltungsdaten und die Zufallsschlüssel; deshalb verläßt der geheime feste Schlüssel nie die Chipkarte.

In den Verwaltungsfeldern 1 und 7 wird z. B. die Geheimhaltungsstufe der in der Datei enthaltenen Datentypen festgelegt, d. h. jede Datentype wird durch eine eigene Geheimhaltungsstufe mit dazugehörigem Schlüssel charakterisiert. Es gibt Datentypen, die immer lesbar sein sollen, wie z. B. Notfalldaten. Dann gibt es Datentypen, die nur mit Zustimmung des Patienten gelesen und/oder nur bestimmten Benutzergruppen zugänglich sein dürfen. Welche Daten in welchen Datentyp eingeordnet werden, hängt von den datenschutzrechtlichen Vorschriften der jeweiligen Länder ab. Im Regelfall werden die jeweiligen Datentypen nur bestimmten Benutzergruppen zugreifbar sein. Zum Beispiel sollen Apotheker nur auf Daten zugreifen können, die sie für ihre Tätigkeit benötigen. In den Verwaltungsfeldern werden die berechtigten Benutzergruppen, die Zugang zu dem jeweiligen Datentyp haben, festgelegt. Zum Beispiel kann festgelegt werden, daß die Apotheker nur auf Rezepte und Hinweise von Ärzten auf Kontraindikationen zugreifen können. Es können daher beispielsweise folgende Datentypen festgelegt werden:

Datentyp 0 — Daten sind immer lesbar — Daten sind nicht verschlüsselt.

Datentyp 1 — Daten sind nur nach Eingabe der PIN-Nummer des Patienten lesbar.

Datentyp 2 — Daten können nur nach Authentisierung vom Arzt eines beliebigen Fachgebietes und nach Eingabe der Patienten-PIN gelesen werden.

Datentyp 3 — wie Datentyp 2; hier kommt hinzu, daß die Daten nur von einem Arzt eines bestimmten Fachgebietes gelesen werden können.

Datentyp 4 — Für spätere Benutzung reserviert.

Datentyp 5 — Die Daten können z. B. sowohl von einem Arzt und einem Apotheker usw. gelesen werden ohne daß die Patienten-PIN erforderlich ist. Dieser Datentyp kann an Mitglieder einer bestimmten Gruppe gerichtet sein, z. B. nur an Röntgenfachärzte, Apotheker oder an alle. Es können auch mehrere exakt spezifizierte Zielgruppen als Liste angegeben werden.

Die genannten Datentypen werden im Datensatz getrennt voneinander abgelegt. Außerdem müssen Daten verschiedener Facharztgruppen oder Daten, die nur für eine bestimmte Zielgruppe gedacht sind, jeweils in getrennten Dateien gehalten werden.

Zu jedem Datensatz gehören Verwaltungsdaten, aus denen unter anderem der Datensatztyp (Notfalldaten/Apothekerdaten/klinische Daten), die enthaltenen Datentypen 0..5, die Fachrichtung des Arztes, der den Datensatz geschrieben hat, sein Name, seine Identifizierung, Datum, Zeit sowie die Zielgruppe der Daten, hervorgehen. Die Zielgruppe, welche die Daten lesen darf, kann auch mit "alle" gekennzeichnet sein. Jeder Datentyp ist mit einem eigenen Zufallsschlüssel verschlüsselt. Diese Zufallsschlüssel und ein Teil der Verwaltungsdaten, der geschützt werden soll, werden ihrerseits mit einem festen, auf der Chipkarte gespeicherten Schlüssel verschlüsselt. Die Chipkarte selbst verschlüsselt die Verwaltungsdaten und die Zufallsschlüssel; deshalb verläßt der geheime feste Schlüssel nie die Chipkarte. Nur der Chip selbst entschlüsselt die Verwaltungsdaten und Zufallsschlüssel, nachdem er geprüft hat, ob der Arzt entweder für die in den Verwaltungsinformationen enthaltene Zielgruppe authentisieren konnte. Gehört der Arzt nicht dieser Zielgruppe an, darf er nur mit Einverständnis des Patienten auf diese Daten zugreifen.

Fig. 2 beschreibt in der Form eines Flußdiagramms die einzelnen Schritte beim Lesen und Schreiben der Daten. Voraussetzung für das Lesen und Schreiben von Daten mittels des erfindungsgemäßen Systems/Verfahrens sind Patientenkarte, Benutzerkarte, Lese-/Schreibgerät und ein Computersystem zur Steuerung des Verfahrens. Als Patientenkarte eignet sich insbesondere die optische Chipkarte. Es kommt auch jede andere Chipkarte in Betracht. Diese Patientenkarte besteht vorzugsweise aus einem optischen Massenspeicher und einem Chip, der die kryptographischen Funktionen enthält. Der Chip einer optischen Chipkarte dient weiterhin als der geschützte Nachrichtenweg, auf dem zwei Parteien Schlüssel übertragen können, weil er Schlüssel sicher aufbewahrt. Jede Patientenkarte enthält ihren eigenen Satz Schlüssel, die nicht einmal dem Kartenherausgeber bekannt zu sein brauchen. Die Patientenkarte gibt die Schlüssel nie nach außen. Die Patientenkarte blockiert die Ver- und Entschlüsselungsfunktionen solange, wie sich ein Arzt ihr gegenüber nicht vorschriftmäßig authentisiert.

Beim Lesen einer Datei muß der Arzt im Besitz einer Benutzerkarte sein. Die Benutzerkarte legitimiert den Arzt als zugelassenen Arzt eines bestimmten Fachgebietes. Die Benutzerkarte wird von einem Lesegerät oder Lese-/Schreibgerät gelesen. Die Benutzerkarte ist technisch nicht bei jeder Legitimation unbedingt erforderlich, da die Benutzergruppeninformation des Arztes bereits im Arztsystem in sicherer Form niedergelegt sein kann. Weiterhin ist erforderlich, daß der Patient seine Patientenkarte in ein Lese/Schreibgerät führt. Ist der Arzt authentisiert, öffnet ihm das System zuerst den Zugriff auf Daten, die jeder Benutzergruppe zugänglich sind. Diese Daten sind auch nicht verschlüsselt (Notfalldaten).

Möchte der Arzt Zugriff auf geschützte Daten, muß die Benutzerkarte die Information enthalten, zu welcher Benutzergruppe der Arzt gehört (z. B. Hautarzt, Lungenarzt usw.). Hierbei entnimmt das System von der Benutzerkarte die entsprechende Information zu, welcher Benutzergruppe der Benutzer gehört, und ruft einen Authentisierungsbefehl der Patientenkarte gegenüber auf. Die Patientenkarte verifiziert, ob der Benutzer zu der behaupteten Benutzergruppe gehört und hält diese Information auf der Patientenkarte. Ein Benutzer kann zu mehreren Benutzergruppen gehören. Das System liest dann eine Datei, die medizinische Daten des Patienten enthält, und trennt die Datei in Datenkopf und Datensatz. Daraufhin wird der Datenkopf mit den Verwaltungsdaten mit einem Entschlüsselungs-Befehl an

die Patientenkarte übertragen. Bevor die Patientenkarte den Datenkopf entschlüsselt, prüft sie, ob eine Authentisierung vorliegt. Im Falle, daß eine Authentisierung vor liegt und der Benutzer mit der Benutzergruppe der Zielgruppe des Datenkopfes identisch ist, gibt sie den entschlüsselten Datenkopf an das System zurück. Das System nimmt den gewünschten Schlüssel aus dem Datenkopf und sendet ihn an die Patientenkarte zur Entschlüsselung. Der entschlüsselte Schlüssel wird an das System zurückgegeben, wobei das System nun mit einem eigenen Entschlüsselungsprogramm den Datensatz des entsprechenden Datentyps entschlüsselt.

Beim Schreiben von Daten ist es genau umgekehrt, mit dem Unterschied, daß die Schlüssel von einem Datenschlüsselgenerator auf der Patientenkarte erzeugt werden. Damit verschlüsselt das System zuerst den Datensatz, wobei jeder Datentyp im Datensatz mit eigenem Zufallsschlüssel verschlüsselt wird. Dann werden die Schlüssel an die Patientenkarte zur Verschlüsselung gesendet. Dann wird der Datenkopf aufgebaut und das System schickt den Datenkopf ebenfalls zur Verschlüsselung an die Patientenkarte.

Das Ergebnis ist ein verschlüsselter Datensatz mit verschlüsseltem Schlüssel und verschlüsselte Verwaltungsdaten, die zum Zugriff auf die Daten auch erforderlich sind.

Zum Beispiel kann festgelegt sein, daß nur Ärzte das Recht haben, auf der Patientenkarte medizinische Daten abzulegen oder daß Apotheker nur ein eingeschränktes Schreiberecht haben und nur ihre fachbezogenen Daten schreiben und lesen können. So können sie ein Rezept löschen, wenn sie ein Medikament verkauft haben, können Anmerkungen zu Hersteller und Chargennummer festhalten und Ähnliches. Der Patient muß immer zuerst zustimmen, bevor der Arzt medizinische Daten auf die Karte schreiben will. Der Arzt hat deshalb die Verantwortung, dem Patienten zu erklären, was er auf die Karte schreiben möchte, damit der Patient hierzu seine Zustimmung/Ablehnung geben kann.

Wenn ein Arzt Daten auf eine Patientenkarte schreiben möchte, muß er sich als Arzt authentisiert haben. Dies geschieht wie beim Lesevorgang durch die Benutzerkarte. Aus der Benutzerkarte ergibt sich auch die jeweilige Facharztgruppe. Der Patient muß sich durch Eingabe seiner PIN-Nummer ebenfalls als berechtigte Inhaber der Patientenkarte legitimiert und seine Zustimmung gegeben haben, bevor der Arzt eine Datei schreiben kann. Anhand des verwendeten Authentisierungsschlüssels stellt die Patientenkarte fest, daß es sich um einen Arzt einer bestimmten Facharztgruppe handelt. Ein Arzt kann auch im Besitz mehrerer Authentisierungsschlüssel sein, wenn er Facharzt in mehreren Gebieten ist.

Dieser verschlüsselte Datensatz mit verschlüsselten Schlüssel und verschlüsselten Verwaltungsdaten kann nun auf optische Speichermedien oder den Chip der Optischen Speicherkarte geschrieben werden, in einem Computer gespeichert werden oder über ein Netz versendet werden. Ein Arzt kann nur unter Mitwirkung derselben Patientenkarte wieder auf die Daten zugreifen. Es besteht auch die Möglichkeit, die Daten von einer optischen Chip-Karte zu archivieren und bei Verlust der Originalkarte ein Duplikat herzustellen.

Fig. 3 zeigt den grundsätzlichen Aufbau eines Informations- und Übertragungssystems für die Speicherung und Übertragung von schützbaren Daten, insbesondere Patientendaten. Das System besteht im wesentlichen aus einem Computer, einem Schreib-/Lesegerät für die Patientenkarte, einer Patientenkarte, einem Schreib-/Lesegerät für die Benutzerkarte und einer Benutzerkarte. Es ist technisch ebenfalls möglich, sowohl für die Patientenkarte als auch die Benutzerkarte ein einziges Schreib/Lesegerät einzusetzen. Die Patientendaten werden entweder auf der Patientenkarte gespeichert oder können auf jedem anderen beliebigen Speichermedium niedergelegt werden. Im Falle, daß die Patientendaten auf der Patientenkarte niedergelegt sind, wird vorzugsweise ein optischer Massenspeicher eingesetzt. Die Patientenkarte ist vorzugsweise eine Chipkarte mit einem optischen Massespeicher. Sie ist immer zum Schreiben und Lesen von Daten notwendig. Auf der Patientenkarte sind folgende wesentliche Daten/Funktionen niedergelegt: Authentisierungsschlüssel für die jeweiligen Benutzergruppen, Verschlüsselungsschlüssel für die Datenschlüssel, Verschlüsselungsschlüssel für den Datenkopf, Generator für die Erzeugung von Datenschlüssel und Ver- und Entschlüsselungsfunktionen.

Die vorliegende Erfindung wurde am Ausführungsbeispiel Patientenkarte ausführlich beschrieben. Es ergibt sich jedoch ohne weiteres, daß das erfindungsgemäße System/Verfahren auch auf alle schützenswerten Daten angewandt werden kann, wo ein eingeschränktes Zugriffsrecht auf bestimmten Daten einer Person, Unternehmens, Bank, einer Behörde oder sonstigen Einrichtung eingeräumt werden soll. Dies gilt insbesondere für Anwendungen mit folgenden Rahmenbedingungen:

- der Eigentümer von Daten verschiedene Sicherheitsstufen einrichten und verwenden kann,
- die Daten jeweils nur einer bestimmten Zielgruppe oder einer Anzahl von Zielgruppen zugänglich gemacht werden sollen,
- bei bestimmten Sicherheitsstufen eine Authentisierung des Leseberechtigten erzwingen kann (z. B. mit der Benutzerkarte),
- bei bestimmten Sicherheitsstufen eine Identifikation und Zustimmung des Chipkartenbesitzers, z. B. über eine PIN-Eingabe, erzwingen kann.

Als Beispiel für die Anwendung der vorliegenden Erfindung kommt eine Chip-Bankkarte in Betracht, in der die Anlagewerte einer Person oder Firma niedergelegt sind. So könnte der Inhaber dieser Chip-Bankkarte den jeweiligen Banken nur ein eingeschränktes Zugriffsrecht einräumen. Als weiteres Beispiel käme auch eine Chip-Kreditkarte in Betracht. Die vorliegende Erfindung kann daher ohne jegliche Änderung des erfindungsgemäßen Verfahrens/Systems auf alle Anwendungen zur Speicherung und Übertragung von schützbaren Daten angewandt werden.

Die vorliegende Erfindung wird nochmals kurz zusammengefaßt. Die auf der Patientenkarte gespeicherten Daten werden durch kryptographische Methoden geschützt. Nur dieselbe Patientenkarte kann die Daten wieder entschlüsseln, wenn sich ein Arzt authentisiert und der Patient zugestimmt hat. Alle Informationen, die die Patientenkarte braucht, um zu entscheiden, ob der Arzt authentisiert ist, und die Schlüssel zum Schutz der Verwaltungsdaten und Zufallsschlüssel sind im Chip enthalten. Die Patientendaten können, müssen aber nicht, auf dem Chip niedergelegt sein. Der Chip kontrolliert sowohl den Zugriff auf die Daten als auch die Ver- und Entschlüsselungsfunktionen. Zufallsschlüssel, die ihrerseits verschlüsselt zusammen mit den Daten gespeichert werden, stellen sicher, daß jeder Datensatz vom anderen getrennt bleibt und daß nur autorisierte Perso-

nen zugreifen können. Jede Patientenkarte hat ihren eigenen Satz Schlüssel. Sollte der Zufallsschlüssel für einen Datensatz gebrochen werden, bleiben die anderen Datensätze auf der Karte sowie alle anderen Karten im System davon unberührt. Wenn der Schlüssel zum Verschlüsseln der Zufallsschlüssel einer Patientenkarte gebrochen würde, wären die Daten aller anderen Karten im System weiterhin sicher.

Die zur Authentisierung verwendeten Schlüssel in den Patientenkarten sind von einem Merkmal der Patientenkarte abgeleitet und daher in jeder Patientenkarte unterschiedlich. Wenn eine Patientenkarte gebrochen würde, lägen damit immer noch nicht die im System verwendeten Schlüssel selbst offen.

Angehörige der Heilberufe authentisieren sich gegenüber der Patientenkarte mit ihrer Benutzerkarte. Die Benutzerkarte enthält einen Satz Gruppenschlüssel, die der Systembetreiber definiert. Nur wenn sich ein Arzt mit einem Schlüssel authentisiert und der Patient mit seiner PIN-Nummer zugestimmt hat, kann der Arzt auf die Daten zugreifen. Die Gruppenschlüssel unterscheiden sich entsprechend ihren Aufgaben im Heilberuf und nach ärztlicher Fachrichtung.

Daten können je nach Schutzbedürfnis unterschiedlich klassifiziert werden. Die Klassen unterscheiden sich darin, ob eine Authentisierung der Benutzer erforderlich ist oder nicht und ob der Patient zustimmen muß oder nicht.

Patentansprüche

1. Speicher- und Informationsübermittlungssystem zumindest enthaltend
ein Computer, verbunden mit
einem Authentisierungsterminal, mittels dessen eine Authentisierung eines Benutzers ausführbar ist,
ein Schreib-/Leseterminal, mittels dessen Daten zwischen dem Computer und einer Chipkarte, die einem Inhaber zuordenbar ist, austauschbar sind, und
mindestens ein Speichermedium,
wobei zwischen dem Computer und dem Speichermedium Daten austauschbar sind, **dadurch gekennzeichnet,** daß eine Chipkarte mit einem Generator enthalten ist, mittels dessen bei jeder Anforderung eines kryptografischen Schlüssels durch den Computer jeweils ein neuer kryptografischer Schlüssel erzeugbar ist.

2. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß
ein Identifikationsterminal enthalten ist, welches mit dem Computer verbunden ist,
wobei mittels des Identifikationsterminals eine Sicherung, insbesondere ein Paßwort oder eine persönliche Identifikationsnummer oder biometrische Identifikationsmethoden, des Inhabers der Chipkarte eingebbar ist.

3. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß eine Authentisierungskarte, mit deren Hilfe die Authentisierung ausführbar ist, enthalten ist.

4. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das Speichermedium auf der Chipkarte angeordnet ist.

5. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das Speichermedium als Festplattenspeicher ausführbar ist.

6. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das Speichermedium als optischer Speicher ausführbar ist.

7. Speicher- und Informationsübermittlungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das der Computer in einem Computer-Netzwerk angeordnet ist und das Speichermedium einem beliebigen Computer im Netz zugeordnet ist.

8. Verfahren zum Speichern von Informationen auf mindestens einem Speichermedium mit Hilfe einer Chipkarte, enthaltend folgende Schritte:
Authentisieren eines Benutzers mittels eines Identifikationsmerkmals, der einer Benutzergruppe zugeordnet ist,
Anfordern eines oder mehrere kryptographischen Schlüssel durch einen Computer von der Chipkarte,
Übertragen des(der) kryptographischen Schlüssels von der Chipkarte zu dem Computer,
Verschlüsseln von Daten mittels des kryptografischen Schlüssels in dem Computer,
Verschlüsseln des kryptographischen Schlüssels in der Chipkarte und
Speichern des verschlüsselten Datensatzes mit den verschlüsselten Schlüsseln im Speichermedium.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Authentisierung mittels eines Authentisierungsterminals, welches mit dem Computer verbunden ist, und einer Authentisierungskarte, die in das Authentisierungsterminal eingeführt wird, ausgeführt wird.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß eine Sicherung, insbesondere eine persönliche Identifikationsnummer oder ein Passwort oder biometrische Identifikationsverfahren, eingegeben werden.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß die Sicherung eingegeben werden kann, bevor die Chipkarte Ver- bzw. Entschlüsselungsfunktionen ausführt.

12. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der kryptographische Schlüssel mit Hilfe eines Kartenschlüssels verschlüsselt wird, wobei der Kartenschlüssel auf der Chipkarte angeordnet ist.

13. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß im Computer zu jedem Datensatz ein Datenkopf erzeugt wird, wobei dem Datenkopf insbesondere zu entnehmen ist, welcher Benutzergruppe der Schreibende zugeordnet wird oder welche Anforderungen zum Lesen des Datensatzes vorliegen müssen.

14. Verfahren nach den Ansprüchen 12 und 13, dadurch gekennzeichnet, daß der mittels des Kartenschlüssels verschlüsselte kryptographische Schlüssel in dem Datenkopf angeordnet wird.

15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß der verschlüsselte Datenkopf und der verschlüsselte Datensatz zu einer Datei zusammengefügt werden und diese Datei in dem Speichermedium gespeichert wird.

16. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der Computer in einem Computernetzwerk angeordnet ist, und das Speichermedium einem beliebigen Computer im Netz zugeordnet ist.

17. Verfahren zum Lesen von Informationen von einem Speichermedium mit Hilfe einer Chipkarte,

enthaltend folgende Schritte:

Authentisieren eines Benutzers mittels eines Identifikationsmerkmals, der einer Benutzergruppe zugeordnet ist.

Übertragen einer Datei von dem Speichermedium auf den Computer,

Trennen der Datei in einen Datenkopf und einen verschlüsselten Datensatz,

Übertragen des Datenkopfes vom Computer auf die Chipkarte,

Entschlüsseln des Datenkopfes mittels eines Kartenschlüssels auf der Chipkarte,

Übertragen des entschlüsselten Datenkopfes von der Chipkarte zu dem Computer,

Ermitteln der Zielbenutzergruppe aus dem entschlüsselten Datenkopf,

Entschlüsseln des verschlüsselten Datensatzes mittels eines kryptographischen Schlüssels, wenn die Benutzergruppe des Benutzers und die Zielbenutzergruppe des Datenkopfes identisch sind und/oder sonstige frei bestimmbare Zugriffsbeschränkungen erfüllt sind.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 196 29 856 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 29. Januar 1998

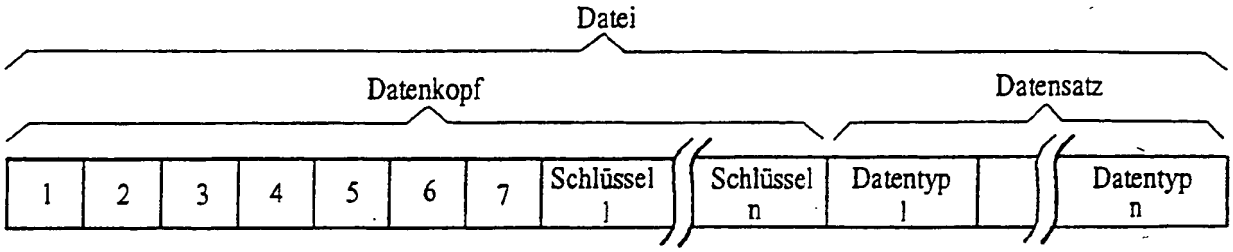


FIG. 1

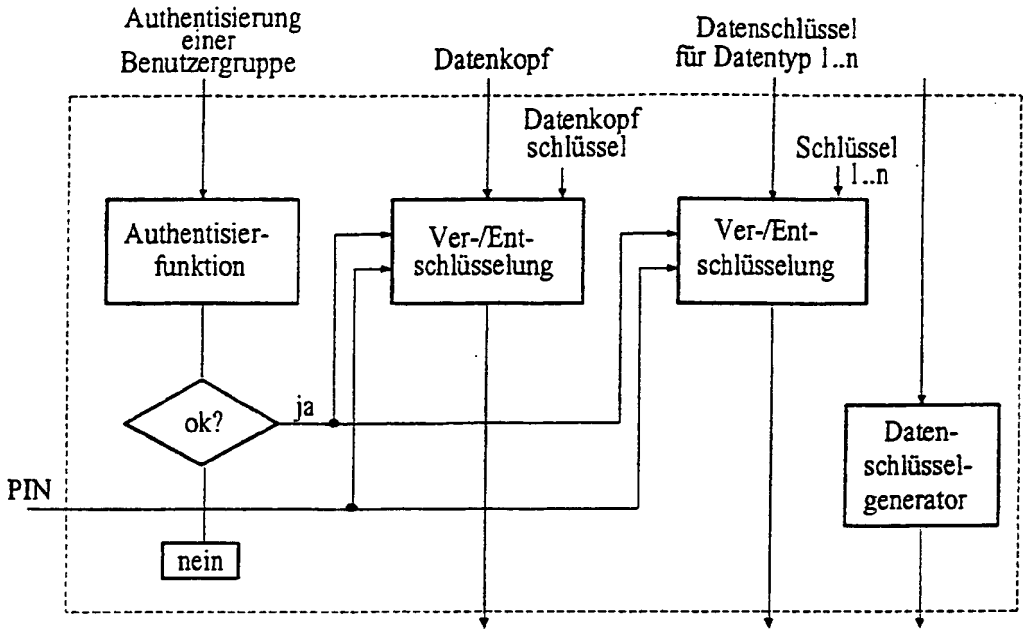


FIG. 2

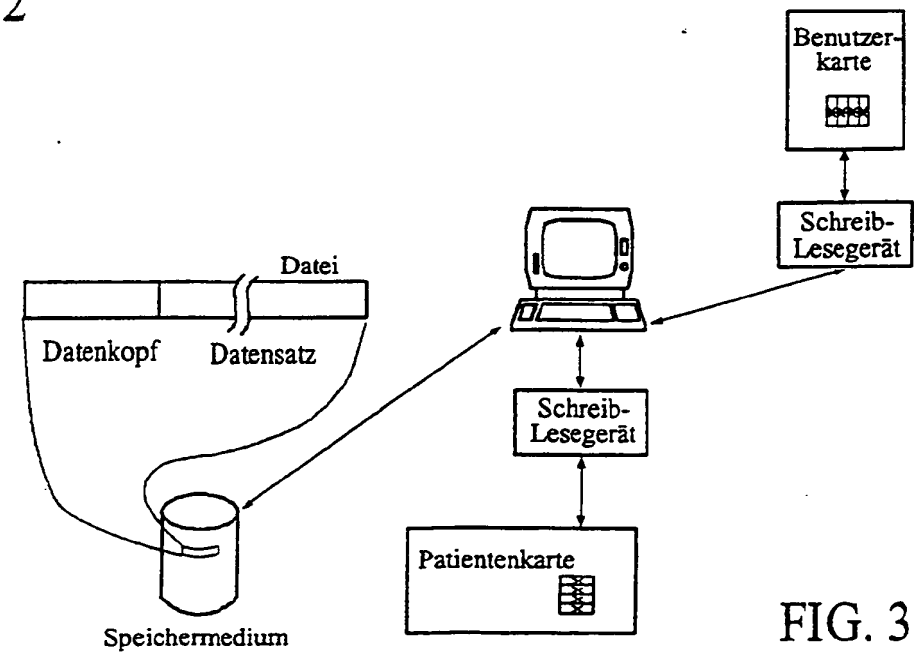


FIG. 3